Phoenix Contact GmbH &Co

Single-signal transmission of safe process information

Description

The invention relates to a method and an apparatus for transmission of safe process signals between input and output units in a safety system.

Particularly in the case of systems which comprise standardized networks and have to satisfy stringent safety requirements, such as SIL 3 according to IEC Standard 61508 or, for example, Safety Category 4 in accordance with EN 954-1, the external circuitry of, for example, sensors and actuators must be designed on the basis of two channels, in order to ensure the necessary safety by means of the redundancy.

Such two-channel external circuitry is conventionally passed in the case of safety systems to similarly comparable, other redundant external circuitry, via separate signals from the sensors, which signals are normally transmitted via input/output units using a network or backplane bus of an integrated computer for control and/or logic processing. The control and/or logic processing then processes the two-channel signal circuitry by means of an appropriately matched emergency-off functional component, which must therefore furthermore be designed to have two channel inputs, and in consequence initiates a safe reaction. The safe reaction is often carried out directly at the controller, or is transmitted by means of a network and/or a backplane bus for

the system-integrated computer to a corresponding output assembly, for example to an actuator.

The object of the invention is to indicate a way in which the transmission and, in consequence, the processing of safe process information are ensured in a considerably simplified manner, in particular in conjunction with an additional increase in the amount of data which can be transmitted and/or can be processed without any loss of information, and which in consequence allows better utilization of the system capacity.

In a very surprising manner, the solution according to the invention is achieved simply by a method having the features of claim 1, by an apparatus having the features of claim 11, and by a system having the features of claim 20.

Advantageous and/or preferred embodiments and developments are the subject matter of the respective dependent claims.

The invention therefore provides that, for transmission of safe process information, two or more process signals, which are detected redundantly in order to identify an event which is relevant to system safety, are converted to a single process signal for system-based further processing.

The invention thus ensures that, particularly when using an apparatus for safe transmission of process signals which are detected redundantly for system safety, which apparatus has means for conversion of process signals, which are carried on two or more channels, to a single process signal which can be tapped off from one output channel, there is a substantially smaller amount of data to be transmitted and consequently to be further processed, for the same overall information content.

Furthermore, the invention makes it possible to achieve the reduction from a multichannel configuration of signal carrying paths, which would otherwise be required for safe transmission and system-based further processing of safety-relevant signals which are detected redundantly, to signal carrying paths in the form of single channels within the system. The hardware and/or software elements which are used for transmission and/or further processing of the safety-relevant process information in the system can thus be produced in a simplified and thus more cost-effective manner. Furthermore, the simplification obtained in this way, in particular as a result of the representation of the actual signal content that this makes possible, allows considerably simplified configuration and programming of safe systems.

In one advantageous development, the conversion is carried out to a digital signal, in particular in order to ensure further-simplified and faster, processor-based further processing of the process signal in order to initiate very highly time-critical reactions.

If, in one advantageous development, the conversion means comprises an A/D converter, this furthermore ensures the detection and/or transmission both of digital and/or analog process signals relating to externally connected device components so that, essentially, any commercially customary or available safety components, such as an emergency-off component or a sensor for area monitoring for optical gratings, guard doors or scanners, can be connected to the system in order to supply safety-relevant process information.

A further preferred embodiment provides for the useful content of the converted process signal to be transmitted in

the form of a 1-bit data item, which can be provided on an application-specific basis, for example just by using a single logic "AND" gate. A core safety system, once it has been configured and/or brought into operation, is in consequence independent of any replacement or of any changes to input and/or output components which can be connected and are relevant to system safety.

In order to further improve safety, the invention furthermore proposes that the transmission of the converted process signal be protected, in particular by means of a data protection value, which is based on the useful content, wherein, in a further advantageous embodiment, the means for protection of the converted signal is designed for generation and attachment of at least one check bit that follows the useful content.

In this case, the use of a so-called CRC (cyclic redundancy check) has been found to be particularly expedient in practice in order to further significantly improve the error identification rate.

The conversion means, which preferably comprises hardware and/or software elements, can advantageously be included at essentially any point, which is and/or can be predetermined as desired, in a process signal transmission path, so that, in particular, this ensures that the safety system can be extended even subsequently by means of additional safety-relevant components.

In consequence, the invention can essentially be used in any desired networks and allows safety-relevant components to be arranged distributed over the entire network, irrespective of system-based units such as system couplers and gateways, and is distinguished by a high level of simple integration, even

using existing technologies.

One advantageous development furthermore additionally provides that, in addition, the process signal which is converted to a single channel for safe system processing is also converted once again to two or more process signals, which, in particular, are carried via separate channels, in system output assemblies which are and/or can be predetermined, such as system-specific actuators, drives or mechatronics units.

The invention will be described in more detail in the following text using a preferred embodiment and with reference to the attached drawing, in which:

Figure 1 shows a highly simplified block diagram of a safety system with an emergency-off safety input component connected to it, and

Figure 2 shows an outline sketch relating to a signal chain for a safety function according to the invention.

A safety system which is identified overall by 1 is illustrated in a greatly simplified form with reference first of all to Figure 1, with this safety system being used, for example, to control and/or regulate safety functions relating to personnel, machines and/or environmental protection in the manufacturing industry.

For this purpose, by way of example, an emergency-off functional component 2 is connected to a safe input component 11 of the safety system 1 in order to identify an "emergency-off" event which is relevant to system safety and which may, for example, be provided for a drive that is to be monitored. Particularly in the case of existing stringent safety

requirements, as mentioned above, the circuitry of an emergency-off functional component 2 such as this must be designed redundantly, for example with two channels. In the present example, in the case of the illustrated emergency-off function that is not activated, two contacts K_{21} and K_{22} which are arranged in parallel are in the contact-making state, so that the partial signal paths S_{211} and S_{212} which are associated with the contact K_{21} are conductively connected to one another via the closed contact K_{21}. In this case, a "one" signal, which is associated with the contact K_{21}, can be tapped off at the safe system input component 11. A "one" signal which is associated with the contact K_{22} can be tapped off in a corresponding manner by means of the safe input component 11 at the partial signal paths S_{221} and S_{222} which are connected to one another.

When the emergency-off function is operated by pushing an emergency-off button 22 in the direction identified by A in Figure 1, the contacts K_{21} and K_{22} are opened, so that, in consequence, a "ZERO" signal, which is associated with the contact K_{21} can thus be tapped off at the input component 11 via the signal path S_{211}-S_{212}, which is thus interrupted, and a "ZERO" signal which is associated with the contact K_{22} can be tapped off via the interrupted signal circuit S_{221}-S_{222}.

The two process signals which are detected redundantly for safety are now, according to the invention, reduced to a single process signal S_1 by means of the safe input component 11 of the safety system 1. The sole process signal S_1 is thus passed via a network (which is not illustrated in any more detail) and/or a backplane bus of a system computer and via a channel to the system-based further processing of a controller 12, with appropriately designed logic processing. If a safe reaction is to be initiated in response to the process signal S_1, this is carried out directly at the

controller 12 or is transferred by means of the network and/or backplane bus further to a safe output component 13 which, via reaction signals S_{14} and S_{15}, appropriately drives microcontrollers 14 and 15, respectively, in order to switch off associated area devices which are monitored by the safety system 1, that is to say in the present case drives to be monitored, for example motors or guard doors.

The conversion is preferably carried out to a digital signal S_1 in particular in order to ensure processor-supported further processing, at least virtually online, of the process signal S_1.

In order to generate a 1-bit data item, the safe input component 11 in the example on which this is based preferably comprises a logic "AND" operation, which is formed by means of appropriate hardware and/or software elements, for the two signal channels S_{211}-S_{212} and S_{221}-S_{222}.

In a corresponding manner, the converted process signal S_1 has the value "1" when both the switches S_{21} and S_{22} are closed, and two associated redundant process signals can thus be tapped off, each having a signal content which corresponds to the signal value of "1", via the safe input component 11. If the emergency-off function is activated and both signal paths S_{211}-S_{212} and S_{221}-S_{222} are thus interrupted, the converted process signal S_1 has the value "0". In a corresponding manner, the signal value of the process signal S_1 corresponds to the value "0" when one of the two switches S_{21} and S_{22} is opened, so that the signal value of the process signal S_1 is thus always "0" in a fault situation or safety situation.

The reduction of the redundantly detected process signals to the single process signal S_1 thus relates exclusively to the number of channels and not to the overall signal content. If,

for example as shown in Figure 1, monitoring for short-circuits is carried out, then in the case of the system-based further processing according to the invention with the single-channel system between the safe input component 11 and the output component 13 of the safety system 1, the overall signal content which signals a fault-free behavior is in consequence based on the signal values "both channels 1" which are valid in this case for S_{211}-S_{212} and S_{221}-S_{222} .

In order to improve safety, the process signal S_1 is furthermore transmitted in a protected manner between the safe input component 11, which is illustrated in Figure 1, and the safe output component 13.

In practice, at least one check bit or one check sum is attached to the useful content for this purpose, by means of the input component 11. The safe input component 11 preferably comprises a means, for example an appropriately adapted shift register, for carrying out a CRC method. The CRC code to be generated is generated at an appropriately high level depending on the application and/or requirements specific to the safety system and relating to the protection respectively required, for example using a CRC-32 code. However, it should be mentioned that suitable safety measures can also be carried out by other means which are known per se to the person skilled in the art, in order in particular, to satisfy the IEC International Standard 61508.

With additional reference to Figure 2, a signal chain according to the invention thus first of all comprises safe detection of input information based on functional components 100 such as sensors which can be connected and which initiate safety-relevant events. The events and process information which is or are in each case detected by means of redundant process signals S_{100} is or are then in each case converted via

safe input components 100 to a single process signal S_{110} for further system-based processing. It should be mentioned that the process signals S_{100} to be converted, that is to say those present at the input of the input components 110, are in digital and/or analog form, depending on the specific application or protection function component. In order to allow the input components 110 to convert analog process signals S_{100} to a digital process signal S_{101}, the conversion device has an appropriate A/D converter component.

Furthermore, it should be mentioned that the conversion devices 110 may also be contained in intelligent network subscriber components or mechatronic units, depending on the system-specific embodiment, and need not necessarily be in the form of separate safe input components.

The process signals S_{110}, which are provided in their protected form downstream from the conversion devices 110, may in consequence be transported on a single channel through the entire system, that is to say in particular via at least one ring, star, line and/or tree network and/or bus network including transmission paths and structure/processing components.

Furthermore, the converted process signal is in consequence processed on a single channel in the system-based further-processing devices 120, such as controllers and/or logic devices and/or networks.

In order to initiate safe reactions in response to respective process signals S_{110}, corresponding reaction signals S_{120}, which are preferably also provided in the form of single signals and in a protected form, are passed to corresponding output components 130 which in the present case are designed for binary signal processing, in order to drive connected

output functional components 140, such as actuators, in particular drives and/or mechatronic units, in accordance with the initiated reactions, for safe output and/or for safe disconnection.

As is indicated in Figure 2, the invention furthermore covers embodiments in which the safe output components 130 are at least partially also designed such that a process signal S_{120} which is supplied on a signal channel and has protected process information is once again converted to two more process signals S_{130}, which can also be transmitted via separate channels, in order to drive the output functional component 140.

The application according to the invention for simplified transmission of safe process information thus allows significant simplification of the configuration and programming of safe systems, in addition to significantly improving the capacity utilization since the amounts of data that have to be transmitted safely are less for the same information content. This is based in particular on the fact that the logic operations which otherwise have to be carried out in hardware on two or more channels are now, on the basis of the invention, carried out on a single-signal basis, representing the actual useful content, which very largely corresponds to the expectation of the engineer, programmer and/or service technician who, for example, identifies the "motor" output as a signal "motor on" or "motor off". A different approach is thus adopted upstream and downstream of the conversion point.

Since the conversion and reduction of two or more process signals, which describe an event which is relevant to system safety, to a single process signal can essentially be carried out at any desired point in the process signal transmission

path, such as for example also in backplane systems, the invention comprises a large number of embodiments, in which the conversion devices are essentially distributed over the entire safety system and/or network, irrespective of any system couplers and gateways.

Overall, in the case of safety systems, the subject matter according to the invention can be used not only in the manufacturing industry, in particular for monitoring emergency-off functions, areas such as optical gratings, guard doors and/or scanners, and various applications, such as robots, area junctions including muting, blanking and/or pressing, and for safety control and/or regulation of actuators and sensor systems, in particular with integrated safety, but can also be used in particular in the field of passenger transport, for example for mountain railroads or lifts, in building engineering, for heating systems and for the process industry, to quote just a few application examples.

In consequence, single-channel safety-relevant process information which is protected, preferably exclusively, on the basis of the safety-relevant pre-processing functions carried out in the conversion devices 110, 130 according to the present description, is transmitted between the safe, system-specifically intelligent input and output components 110, 130 and the logic processing 120 which controls safety.